REMARKS

Claims 1-41 are currently pending in the subject application, and are presently under consideration. Claims 1-41 are rejected. Claims 1, 20, 31, 36, and 38 have been amended. Claims 14, 15, 22, 23, 35, and 37 have been cancelled. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Rejection of Claims 1-41 Under 35 U.S.C. §103(a)

Claims 1-41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Funk (U.S. 5,721,779) in view of Keene, et al. (U.S. PG Pub. No. 2004/0049294). Claims 1, 20, and 31 have been amended to further emphasize their distinctiveness over the cited art. Claims 36 and 38 have been amended to depend from claim 31. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 1 recites a method of administering access and security on a network having a plurality of computers. A one-way encrypted password file is installed on each computer of the plurality of computers in the network. The one-way encrypted password file includes a plurality of user identifications associated one-way encrypted passwords and associated privileges for each authorized user allowed access to the plurality of computers and the network. A password entered by a user is encrypted via one-way encryption when the user logs into a computer. A match is checked for between the user identification and one-way encrypted password entered by the user and the plurality of user identifications and one-way encrypted passwords stored in the one-way encrypted password file. Access is enabled to data and software contained on the computer and the network permitted by the associated privileges for the user when a match is found. Messages broadcast or multicast within the network are filtered and messages permitted by the user's associated privileges are displayed to the user when a match is found on the one-way encrypted password file. It will be appreciated that the password matching, filtering, and display are performed locally at a given computer.

The master password file can be updated at each of the plurality of computers. Updating the master password file includes attaching a new master password file to a message at a computer accessible by a systems administrator or security officer and encrypting the message containing the master password file using a private key and pass phrase available only to the systems administrator or security officer. The message is transmitted to the plurality of computers and decrypted at each computer using a public key corresponding to the private key.

It is respectfully submitted that neither of the references cited in the Office Action teach the filtering and display of broadcast or multicast messages based upon user privileges, either alone or in combination. In addition, neither of the references cited teach the updating of a master password file at a plurality of computers via an asymmetrically encrypted message from a system administrator.

The Office Action states that Keene provides a teaching of broadcasting and/or multicasting a message based on the ability of an authenticated user with modification privileges in Keene to alter an object on a central server. The Office Action asserts that the altered message is a broadcast message as it provides a form of data exchange between the modifying user and other authenticated users on the network. It is respectfully submitted that this form of exchange does not comprise a broadcast or multicast message. It will be appreciated that the broadcast message of the present invention is not sent solely to authenticated users, but broadcast over the airwaves or sent to all or a plurality of users on a network. A plurality of users, authenticated and unauthenticated, receives every message broadcast across the network, but the messages are filtered at the individual computers to restrict the access according to the user's associated privileges. This differs from the characterization of the Keene patent in the Office Action, as the "message" in Keene is a modification of an object at the central server. No message is sent simultaneously to all users (*i.e.*, broadcast) or even to a plurality of intended recipients (*i.e.*, multicast).

In addition, neither Funk nor Keene teach or suggest a password updating process utilizing asymmetric encryption. In fact, neither Funk nor Keene teach or suggest the use of

asymmetric encryption for any purpose. While Funk addresses one-way encryption schemes, this does not comprise a teaching of asymmetric encryption. Additionally, neither reference teaches or suggests the mass updating of password files from a central server in a network environment. Accordingly, it is respectfully submitted that claim 1 is patentable over the cited art.

Turning to the claims depending from claim 1, the applicant asserts that each dependent claim has its own specific limitations and features that define patentable invention over the prior art. For the sake of brevity, the discussion of certain dependent claims will be omitted. In focusing the discussion on specific claims, a concession of the patentable distinctiveness of the other dependent claims is not intended.

Claim 5 recites spoofing the user into believing that access has been gained to the computer upon request of the systems administrator or security officer, wherein spoofing includes the presentation of false messages and information to the user.

Neither of the cited references teach or suggest spoofing an unauthenticated user into believing that access has been gained in the computer system. The Office Action states that the generation of random signals and authentication values in Funk comprises providing false data to the user. It is respectfully submitted, however, that nothing in Funk teaches or suggests providing false data to a user as to deceive the user into believing that access to the computer has been achieved. The claims recite spoofing the user into believing that access has been gained in the computer system, not simply providing false data. Keene also fails to teach or suggest spoofing an unauthorized user who is accessing the system. Accordingly, it is respectfully submitted that claim 5 is nonobvious and patentable over the cited art.

Claims 8 recites displaying a request for reauthentication at the direction of a system administrator or security officer. Claim 9, which depends from claim 8, requires that this reauthentication take the form of a displayed log-in screen having a position for entry of the user identification and password. The Office Action cites two passages in Funk describing an initial

authentication procedure. The claims, however, discuss reauthentication, requiring an already authenticated user to reenter a user identification and password just to maintain the present connection upon the request of a system administrator. Neither of the cited references discusses such a reauthentication process. It is thus respectfully submitted that claims 8 and 9 are nonobvious and patentable over the cited references.

Claim 11, which depends from claim 9, recites a method further including the following steps. A master password file is accessed on a computer system accessible to the system administrator or security officer. The password is one-way encrypted, and the master password file is searched for a match of the user identification and the one-way encrypted password. Claim 13, which depends from claim 11, adds the following steps. An authenticated user enters a new password. The user identification and password stored on the master password file is reauthenticated. The new password is one-way encrypted, and the user identification and password in the master password file are replaced with the new user identification and the new one-way encrypted file.

Neither Funk nor Keene teach or suggest a password updating process initiated by a reauthentication request by the system administrator or security officer. The Office Action cites a passage within the Funk, discussing the encrypted challenge and response process used in authenticating a user, but does not provide the required teaching. The Office Action does not clarify the relevance of the cited passage, despite the arguments in the prior amendment. Accordingly, claims 11 and 13 are patentable over the cited art.

Claim 20 recites a system to administer access and security on a network having a plurality of computers. The system includes a one-way encrypted password file on each computer in the network. The one-way encrypted password file includes a plurality of user identifications, associated one-way encrypted passwords and associated privileges for each authorized user allowed access to the plurality of computers and the network. A user login module receives a user identification or role and password from a user and logs in the user when a match is found in the one-way encrypted password file. A channel monitoring and filtering

module monitors and receives broadcast or multicast messages within the network and displays the message to the user when the user's associated privileges permit the viewing of the message. A remote auditing module monitors and processes anomalous events which may occur on the computer. The anomalous events include the following: a change in the users' associated privileges, a system disable operation initiated by the user, the expiration of a user's password, the rejection of a message due to an invalid digital signature, a request for remote user re-authentication received from the systems administrator or security officer, a request for a remote user lockout received from the system administrator or security officer, and successful completion of a request for remote loading passwords to a system administrator or security officer.

It is respectfully submitted that claim 20 is patentable over the cited art. Specifically, it is submitted that neither of the references cited in the Office Action teach the filtering and display of broadcast or multicast messages based upon user privileges, either alone or in combination. This deficiency in the art is discussed in detail under claim 1, above. The cited art also fails to teach or suggest a remote auditing module that monitors and processes the anomalous events enumerated in claim 20. The ability to recognize and process these anomalous events allows the system of claim 20 to maintain a secure network in an operating environment in which individual computers within the system are regularly in danger of being compromised. It is respectfully submitted that claim 20 is patentable over the cited art.

Turning to the claims depending from claim 20, the applicant asserts that each dependent claim has its own specific limitations and features that define patentable invention over the prior art. For the sake of brevity, the discussion of certain dependent claims will be omitted. In focusing the discussion on specific claims, a concession of the patentable distinctiveness of the others is not intended.

Claim 29 recites a system in which the password management module attaches a master password file containing complete user identifications, associated one-way encrypted passwords and associated privileges to a message, encrypts the message using a private key and pass phrase

for the system administrator or security officer and broadcasts the message to all users. Neither of the cited references contains such a teaching. The Office Action cites a passage in Funk discussing its challenge protocol in rejecting this claim. The cited passage does not address updating of passwords on individual computers in a network. Similarly, neither Keene nor Funk teach or suggest the use of asymmetric encryption. Accordingly, it is respectfully submitted that claim 29 is nonobvious and patentable over the cited art.

Claim 30 recites a system in which the password management file decrypts a message using a public key corresponding to the private key, reports to the system administrator any failure to decrypt the message and replaces the one-way encrypted password file with the decrypted master file. The claim further recites notifying a system administrator if it receives a master password file that it cannot encrypt. This is intended to notify the system administrator of any attempts by an intruder to impersonate the system administrator. When the public key for the administrator fails to match the encryption key used for the file, it can be assumed that the file has been tampered with or otherwise falsified. Neither of the cited references teaches or suggests such a verification method. It is thus respectfully submitted that claim 30 is nonobvious and allowable over the cited art.

Claim 31 recites a computer program executable by a computer and embedded in a computer readable medium to administer access and security on a network having a plurality of computers. The computer program includes a one-way encrypted password file on each computer in the network. Each one-way encrypted password file includes a plurality of user identifications, associated one-way encrypted passwords, and associated privileges for each authorized user allowed access to the plurality of computers and the network. A user login code segment receives a user identification or role and password from a user and logs in the user when a match is found in the one-way encrypted password file. A channel monitoring and filtering code segment monitors and receives broadcast or multicast messages within the network and displays the message to the user when the user's associated privileges permit the viewing of the message. A remote control code segment enables a systems administrator or security officer to

take appropriate action when an anomalous event transpires. The appropriate action includes spoofing the user into believing that access has been gained to the computer, including the presentation of false messages and information to the user.

It is respectfully submitted that claim 31 is patentable over the cited art. Specifically, it is submitted that neither of the references cited in the Office Action teach the filtering and display of broadcast or multicast messages based upon user privileges, either alone or in combination. This deficiency in the art is discussed in detail under claim 1, above. Claim 31 further defines over the prior art because the prior art does not teach spoofing an unauthenticated user into believing that access has been gained in the computer system. The Office Action states that the generation of random signals and authentication values in Funk comprises providing false data to the user. It is respectfully submitted, however, that nothing in Funk teaches or suggests providing false data to a user for the purpose of deceiving the user into believing that access to the computer has been achieved. The claim recites spoofing the user into believing that access has been gained in the computer system, not simply providing false data. If this rejection is maintained, it is respectfully requested that the Examiner explain in what manner randomizing a password signal selected by a user constitutes providing false messages and information to the user as to spoof the user into believing that access to the system has been gained. Keene also fails to teach or suggest spoofing an unauthorized user who is accessing the system. Accordingly, it is respectfully submitted that claim 31 is nonobvious and patentable over the cited art.

Dependent claims 2 – 13, 16 – 19, 21, 24 – 30, 32 – 34, 36, and 38 – 41 depend directly or indirectly from one of independent claims 1, 20, and 31. The applicant asserts that these claims are nonobvious and patentable for the reasons discussed above under their respective base claims and for their own unique elements.

For the reasons described above, claims 1 – 13, 16 – 21, 24 – 34, 36, and 38 – 41 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 3/16/05

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVELAND, OHIO 44114-1400
Phone: (216) 621-2234
Fax: (216) 621-4072